UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/365,446	08/02/1999	HIROKAZU OUGI	773-005	1802

7590 01/26/2004

JOSEPH SOFER
SOFER & HAROUN LLP
317 MADISON AVENUE
SUITE 910
NEW YORK, NY 10017

EXAMINER	
MEISLAHN, DOUGLAS J	
ART UNIT	**PAPER NUMBER**
2137	9

DATE MAILED: 01/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/365,446	OUGI ET AL.	
	Examiner	Art Unit	
	Douglas J. Meislahn	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 November 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *7,8,13 and 14* is/are allowed.

6)☒ Claim(s) *1-6, 9-12, 15-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 05 November 2003 that amended the abstract and claims 3-17 and 19-22. Claims 1, 2, and 18 have not been amended.

Claim Objections

2. Claim 22 is objected to because of the following informalities: "firs" in the eleventh line should be spelled correctly. Also, "converted as a key" in the seventh line is grammatically awkward and should be changed (back) to "converted with a key". Other amendments to the claim have clarified this formerly objected-to phrase. Appropriate correction is required.

Response to Arguments

3. Applicant's arguments filed 05 November 2003 have been fully considered but they are not persuasive. With respect to claim 1, applicant posits that Davis does not show that a "transmission side *encrypts an encryption algorithm operated at the transmission side with an encryption algorithm operated at the reception side and transmits the encrypted algorithm to the reception side*". Davis clearly shows the reception of an encrypted package that contains a new encryption algorithm. The sender, by virtue of possessing it, clearly has access to the new encryption algorithm and is thus anticipated as operating it.

4. With respect to claims 20 and 21, applicant argues that Spies et al. do not disclose a notification of the existence of a suitable algorithm. However, Spies et al. do

teach communication with a suitable algorithm, which mandates some type of confirmation as to the applicability of the algorithm. While this might not be within applicant's conceptualization of the invention, it does meet the limitations of the claims.

5. With respect to claims 6 and 12, Spies et al.'s table 1 shows different key lengths associated with different algorithms. Furthermore, applicant has ignored a section cited in Davis. As such, the combination of Spies et al. and Davis does, in fact, render obvious claims 6 and 12, as well as 2-5, 9-11, 15-19, and 22.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by Davis (6058478).

Davis presents a method of updating cryptographic information, including algorithms, in remote devices. In claims 5, 6, and 8, the most succinct description of the method, an upgrade entity generates an upgrade message (claim 5), encrypts the message with the recipient's public key (claim 6), and sends the resulting cryptogram to the remote device. The remote device accesses the cryptogram, which anticipates use of an encryption algorithm at the remote device, authenticates the contents, and

performs the upgrade (claim 5). The upgrade includes deleting a previously existing algorithm and modifying that now-deleted algorithm to update the cryptographic algorithm. As the update is now the entirety of the now-stored algorithm, it is apparent that the now-stored algorithm was sent in the upgrade message.

8. Claims 20 and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Spies et al. (RE38070).

From line 43 of column 15 through line 17 of column 16, Spies et al. detail the selection of an encryption algorithm for use between two entities. This process includes obtaining the identities of the originating and receiving participants, as embodied in their encryption indices. The originating entity arrives at these values internally, and hence they come from the transmission (originating) side. The sum of these indices is shown in Table 1, which reads on applicant's database. The table shows a correspondence between a participant and encryption algorithms available to that entity, thereby anticipating the second clause of claim 20. Spies et al. say that the parties are trying to agree on an encryption algorithm, and hence the determination step is anticipated. The implication that the originating party encrypts data indicates that notification is given that a suitable algorithm exists. With respect to claim 21, the originating participant selects an algorithm and hence information indicating the encryption algorithm has been transmitted to the sender, albeit internally. Reception of a decryptable message constitutes notification at the receiving participant of enabled communications.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claim 2-6, 9-12, 15-19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies et al. in view of Davis.

Spies et al. present a system for encryption algorithm negotiation. A potential sender compares a list of the algorithms supported internally with a list of those supported by the intended recipient. They do not, however, plan a course of action for when different algorithms are used at the sending and receiving sides. Davis presents a method of upgrading encryption parameters in remote entities (see for example claims 5, 6, and 8). His scheme includes an upgrade entity encrypting encryption algorithms under an algorithm operable by the recipient of the encrypted algorithm, thereby upgrading the algorithm while ensuring the security of the algorithm. He also shows, in figure 3, a communication system between two entities where a third trusted party facilitates trust between the two entities. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate Davis' algorithm update system into Spies et al.'s algorithm selection system. As both Spies et al. and Davis indicate, algorithm use is restricted by the locales of both sender and receiver, and hence it is obvious that the upgrade entity of Davis would need to know the identities of both the sender and the receiver. The sender is the only entity

that can be relied upon to know both of these identities. The joint method includes either the sender or receiver getting the updated algorithm; as such, both claims 2 and 18 are rendered obvious. Claim 17 is broader than claim 18, and hence is also rendered obvious.

Davis' fifth claim teaches including signatures within the cryptogram, thus obviating claims 3 and 19. With respect to claim 4, Davis' figure 3, which shows communications flowing from the trusted entity through the sender to the receiver, renders sending the signature with the encrypted algorithm to the sender and then to the receiver obvious.

Regarding claims 5 and 11, the combination of Spies et al. and Davis has already been shown to render obvious receiving the identities of the sender and the receiver from the sender. Spies et al. show a table that reads on applicant's data base. Davis' demonstration of encrypting an algorithm with an algorithm operable by the entity that receives the encrypted algorithm meets the limitations of the last clause of claims 5 and 11.

With respect to claims 6 and 12, which place, in the cryptogram, a key that is based on the update algorithm and an original key assigned to the cryptogram's recipient, Davis talks about altering cryptographic keys in lines 18-25 of column 2. As described in lines 56-65 of column 1, key length is one possible modification. Thus it is obvious to include in the modification instructions a key that is based on an original key as well as the update algorithm. This key, in unaltered state, is stored in the table.

In regards to claims 9, 10, 15, and 16, the upgrade entity in Davis corresponds to applicant's encryption key management station. Spies et al. have also mentioned that a mutually trusted party holds the table used to select encryption algorithms (column 15, lines 57-59). Other aspects of these four claims have already been discussed. The limitations of claim 22 are met by the preceding paragraphs.

Allowable Subject Matter

11. Claims 7, 8, 13, and 14 are allowed.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2137

DJM

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100